(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle

Bureau international





(43) Date de la publication internationale 15 janvier 2004 (15.01.2004)

PCT

(10) Numéro de publication internationale WO 2004/006088 A2

- (51) Classification internationale des brevets7: G06F 9/30
- (21) Numéro de la demande internationale :

PCT/FR2003/002107

- (22) Date de dépôt international: 7 juillet 2003 (07.07.2003)
- (25) Langue de dépôt :

francais

(26) Langue de publication :

français

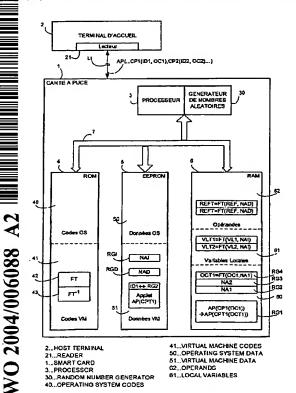
- (30) Données relatives à la priorité: 8 juillet 2002 (08.07.2002) 02/08643
- (71) Déposant (pour tous les États désignés sauf US) : GEM-PLUS [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de GEMENOS, F-13420 GEMENOS (FR).
- (72) Inventeurs; et
- (75) Inventeurs/Déposants (pour US seulement): GIRARD,

Pierre [FR/FR]; 942 Chemin du Tourtaret, F-13112 LA DESTROUSSE (FR). GONZALVO, Benoit [FR/FR]; 2 rue de l'Ecole, F-13600 CEYRESTE (FR).

- (74) Mandataire: MILHARO, Emilien; C/O GEMPLUS, Service brevets, LA VIGIE, PB 90, F-13705 LA CIOTAT CEDEX (FR).
- (81) États désignés (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ. DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) États désignés (régional): brevet ARIPO (GII, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet

[Suite sur la page suivante]

- (54) Title: MAKING SECURE DOWNLOADED APPLICATION IN PARTICULAR IN A SMART CARD
- (54) Titre: SECURISATION D'APPLICATION TELECHARGEE NOTAMMENT DANS UNE CARTE A PUCE



PANDOM NUMBER GENERATOR

- (57) Abstract: The invention concerns a method for differentiating between data and instructions thereby providing against certain attacks in a data processing device such as a smart card, whereby a generator (30) associates a random number with an applicative component of a downloaded application (AP), and a transformer (42) comprised in a virtual machine (VM) applies each of the instruction words (OC1) in the component and the associated random number to a transformation function (FT) so as to store the transformed instruction words (OCT1) when downloading the component. A second transformer (43) applies each of the transformed words (OCT) of part of the component (CP1) and the associated random number (NA1) to the reciprocal function (FT-1) of the transformation function (FT) so as to retrieve the instruction words constituting said component part to execute same.
- (57) Abrégé: Afin de distinguer notamment les données et les instructions et remédier ainsi à certaines attaques dans un dispositif de traitement de données tel que carte à puce, un générateur (30) associe un nombre aléatoire à un composant applicatif d'une application téléchargée (AP), et un transformateur (42) inclus dans une machine virtuelle (VM) applique chacun des mots d'instruction (OC1) dans le composant et le nombre aléatoire associé à une fonction de transformation (FT) afin de mémoriser des mots d'instruction transformés (OCT1) lors du téléchargement du composant. Un autre deuxième transformateur (43) applique chacun des mots transformés (OCT) d'une partie du composant (CP1) et le nombre aléatoire associé (NA1) à la fonction réciproque (FT-1) de la fonction de transformation (FT) afin de récupérer les mots d'instruction composant ladite partie de composant pour exécuter